UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/506,815	04/11/2005	Arvind Ramaswamy	200601202-5	6801

22879 7590 09/01/2010

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
3404 E. Harmony Road
Mail Stop 35
FORT COLLINS, CO 80528

EXAMINER	
ALI, FARHAD	

ART UNIT	PAPER NUMBER
2446	

NOTIFICATION DATE	DELIVERY MODE
09/01/2010	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

JERRY.SHORMA@HP.COM
ipa.mail@hp.com
laura.m.clark@hp.com

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 10/506,815
Filing Date: April 11, 2005
Appellant(s): RAMASWAMY ET AL.

Jonathan M. Harris
(Registration # 44,144)
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 06/21/2010 appealing from the Office action mailed 01/21/2010.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The following is a list of claims that are rejected and pending in the application:

Claims 1-20 are pending.

Claims 1-20 are rejected.

(4) Status of Amendments After Final

The examiner has no comment on the appellant's statement of the status of amendments after final rejection contained in the brief.

(5) Summary of Claimed Subject Matter

The examiner has no comment on the summary of claimed subject matter contained in the brief.

(6) Grounds of Rejection to be Reviewed on Appeal

The examiner has no comment on the appellant's statement of the grounds of rejection to be reviewed on appeal. Every ground of rejection set forth in the Office action from which the appeal is taken (as modified by any advisory actions) is being maintained by the examiner except for the grounds of rejection (if any) listed under the subheading "WITHDRAWN REJECTIONS." New grounds of rejection (if any) are provided under the subheading "NEW GROUNDS OF REJECTION."

(7) Claims Appendix

The examiner has no comment on the copy of the appealed claims contained in the Appendix to the appellant's brief.

(8) Evidence Relied Upon

6,240,091	Ginzboorg et al.	05-2001
6,539,540	Noy et al.	03-2003

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1, 4-11, 13-16, and 18-20 are rejected under 35 U.S.C. 102(e) as being anticipated by Ginzboorg et al. (US 6,240,091 B1) hereinafter Ginzboorg.

Claim 1

Ginzboorg teaches a data network management system for identifying unauthorized access to a data network service **(Column 15 Lines 40-44, "The charging functions correctly when the network access and payments are in synchronization with one another, i.e. when the paying customers have access to the network providing the services and the non-paying customers do not have access")**, said service node having an agent and having means for maintaining a user access list, said user access list having at least one data network address corresponding to at least one user node in said data network **(Column 18 lines 14-24,**

"The router control unit RCU, which includes the router command set, controls the router by handling the maintenance of the aforementioned access list. The synchronization unit SU handles the synchronization of the aforementioned payments and access rights by comparing, at certain intervals, the router's list of open connections to addresses of paying customers. Said addresses are received from the charging server. Any detected conflicts are corrected so that no error longer than said interval can occur in charging"), said system comprising:

a data communication means for periodically polling said agent at said service node and for retrieving a user access list from said agent, said user access list specifying which users have accessed said node **(Column 15 Lines 44-50, "For example, because of a fault the situation may sometimes change so that the router prevents the paying customers from accessing the network providing the services or allows access for non-paying customers (who do not send payment CDRs). To correct such a situation the access server polls the router and the charging server. From the router the access server gets the access list")**;

a database for maintaining an authorized access list for said service node, said authorized access list specifying which users are authorized to access said service node **(Column 15 lines 50-52, "and from the charging server the IP addresses of the customers who pay at the moment in question for access to the network")**; and

a data processing means for detecting unauthorized access to said service node by comparing said user access list to said authorized access list and for updating said authorized access list, based on the user access list retrieved from said agent **(Column 15 lines 50-52, "If the address of a paying customer is not included in the access list, the access server adds the address to the list. If an address included in the access list is not included in the paying customers of the charging server, the access server removes the address from the list. The polling interval can be made to be controllable so that the access service provider can set the desired interval")**.

Claim 4

Ginzboorg teaches the data network management system as defined in claim 1, further including means for installing said agent at said service node, said agent having means to communicate with said data communication means **(Column 5 lines 46-56, "FIG. 3a illustrates how the method according to the invention is applied in a network environment according to FIG. 2. The end user terminal (a personal computer) includes a smart card reader CR and each customer has a personal smart card by which the customer (subscriber) is recognized. Additionally, the terminal includes a program library which communicates with the smart card, and software which generates at specific intervals during the connection (for example, once a minute) a charging record furnished with a digital signature and sends it in the network")**.

Claim 5

Ginzboorg teaches a method for identifying unauthorized access to a data network service **(Column 15 Lines 40-44, "The charging functions correctly when the network access and payments are in synchronization with one another, i.e. when the paying customers have access to the network providing the services and the non-paying customers do not have access")**, provided at a service node in a data network, by a user node in said data network, said service node having an agent and having means for maintaining a user access list, said user access list having at least one data network address corresponding to at least one user node in said data network **(Column 18 lines 14-24, "The router control unit RCU, which includes the router command set, controls the router by handling the maintenance of the aforementioned access list. The synchronization unit SU handles the synchronization of the aforementioned payments and access rights by comparing, at certain intervals, the router's list of open connections to addresses of paying customers. Said addresses are received from the charging server. Any detected conflicts are corrected so that no error longer than said interval can occur in charging")**, said method comprising:

a) periodically polling an agent and retrieving said user access list, for a given period of time, from said service node in said data network **(Column 15 Lines 44-52, "For example, because of a fault the situation may sometimes**

change so that the router prevents the paying customers from accessing the network providing the services or allows access for non-paying customers (who do not send payment CDRs). To correct such a situation the access server polls the router and the charging server. From the router the access server gets the access list and from the charging server the IP addresses of the customers who pay at the moment in question for access to the network");

b) comparing said user access list to an authorized access list; c) determining if an access to said service node was unauthorized based on comparing said user access list to the authorized access list **(Column 15 lines 50-52, "If the address of a paying customer is not included in the access list, the access server adds the address to the list. If an address included in the access list is not included in the paying customers of the charging server, the access server removes the address from the list. The polling interval can be made to be controllable so that the access service provider can set the desired interval")**;

d) if said access was not authorized, initiating a notification process; wherein said user access list identifies a plurality of accesses to said service node **(Column 18 lines 17-24, "The synchronization unit SU handles the synchronization of the aforementioned payments and access rights by comparing, at certain intervals, the router's list of open connections to addresses of paying customers. Said addresses are received from the charging server.**

Any detected conflicts are corrected so that no error longer than said interval can occur in charging").

Claim 6

Ginzboorg teaches the method as defined in claim 5, further including updating said authorized access list based on said user access list retrieved from said service node **(Column 18 lines 14-24, "The router control unit RCU, which includes the router command set, controls the router by handling the maintenance of the aforementioned access list. The synchronization unit SU handles the synchronization of the aforementioned payments and access rights by comparing, at certain intervals, the router's list of open connections to addresses of paying customers. Said addresses are received from the charging server. Any detected conflicts are corrected so that no error longer than said interval can occur in charging").**

Claim 7

Ginzboorg teaches method as defined in claim 5, further including installing said agent at said user node, prior to periodically polling and retrieving said user access list **(Column 5 lines 46-56, "FIG. 3a illustrates how the method according to the invention is applied in a network environment according to FIG. 2. The end user**

terminal (a personal computer) includes a smart card reader CR and each customer has a personal smart card by which the customer (subscriber) is recognized. Additionally, the terminal includes a program library which communicates with the smart card, and software which generates at specific intervals during the connection (for example, once a minute) a charging record furnished with a digital signature and sends it in the network").

Claim 8

Ginzboorg teaches method as defined in claim 5, further including selecting said service node for identification based on a predetermined criteria, prior to retrieving said user access list **(Column 15 Lines 44-50, "For example, because of a fault the situation may sometimes change so that the router prevents the paying customers from accessing the network providing the services or allows access for non-paying customers (who do not send payment CDRs). To correct such a situation the access server polls the router and the charging server. From the router the access server gets the access list")**.

Claim 9

Ginzboorg teaches the method as defined in claim 5, wherein said notification process comprises notifying a Network Operations Console **(See claim 5 rejection "Access server")**.

Claim 10

Ginzboorg teaches the method as defined in claim 5, wherein a) through c) are repeated, and wherein said user node is selected from one of a plurality of user nodes in said data network **(Column 15 Lines 44-52, "For example, because of a fault the situation may sometimes change so that the router prevents the paying customers from accessing the network providing the services or allows access for non-paying customers (who do not send payment CDRs). To correct such a situation the access server polls the router and the charging server. From the router the access server gets the access list and from the charging server the IP addresses of the customers who pay at the moment in question for access to the network" and Column 15 lines 51-52, "The polling interval can be made to be controllable so that the access service provider can set the desired interval")**.

Claim 11

Ginzboorg teaches the method as defined in claim 5, wherein a) through d) are repeated, and wherein said user node is selected from one of a plurality of user nodes

in said data network **(Column 15 lines 51-52, "The polling interval can be made to be controllable so that the access service provider can set the desired interval")**.

Claim 13

Claim 13 is rejected for the same reasons as claim 5.

Claim 14

Ginzboorg teaches the computer-readable medium as defined in claim 13, further containing computer-readable and computer-executable instructions which perform a step of updating said authorized access list based on user access information **(Column 18 lines 14-24, "The router control unit RCU, which includes the router command set, controls the router by handling the maintenance of the aforementioned access list. The synchronization unit SU handles the synchronization of the aforementioned payments and access rights by comparing, at certain intervals, the router's list of open connections to addresses of paying customers. Said addresses are received from the charging server. Any detected conflicts are corrected so that no error longer than said interval can occur in charging")**.

Claim 15

Ginzboorg teaches the computer-readable medium as defined in claim 13, further containing computer-readable and computer-executable instructions which perform a step of installing said agent at said user node, prior to retrieving said user access list in step a) **(Column 5 lines 46-56, "FIG. 3a illustrates how the method according to the invention is applied in a network environment according to FIG. 2. The end user terminal (a personal computer) includes a smart card reader CR and each customer has a personal smart card by which the customer (subscriber) is recognized. Additionally, the terminal includes a program library which communicates with the smart card, and software which generates at specific intervals during the connection (for example, once a minute) a charging record furnished with a digital signature and sends it in the network")**.

Claim 16

Ginzboorg teaches the computer-readable medium as defined in claim 13, further containing computer-readable and computer-executable instructions wherein said steps a) through c) are repeated, and wherein said user node is selected from one of a plurality of user nodes in said data network **(Column 15 lines 51-52, "The polling interval can be made to be controllable so that the access service provider can set the desired interval")**.

Claim 18

Claim 18 is rejected for the same reasons as claim 1.

Claim 19

Ginzboorg teaches the data network as defined in claim 1, wherein said authorized access list is a common authorized user access list, that includes a range of user nodes for comparing to said user access list to determine if said user access list is a subset of said common authorization access list **(Column 9 lines 31-40, "This can be a drawback if the charging server and the access server belong to different organizations. This possible drawback can be "fixed" in the following manner. The customer identifier is formed of two parts. The first part identifies the customer origin (i.e. the customer's own charging server). This part is used to route the START message to the charging server in question. The second part is encrypted by using the public key of the customer's own charging server so that it is not recognized by the access server")**.

Claim 20

Ginzboorg teaches the data network management system of claim 1 wherein said user access list identifies a plurality of accesses to said service node **(See claim 1 rejection)**.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 2-3, 12, and 17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ginzboorg in view of Noy et al. (US 6,539,540 B1).

Claim 2

Ginzboorg teaches the data network management system as defined in claim 1.

Ginzboorg does not specifically disclose wherein said agent is a Simple Network Management Protocol agent.

However, Noy et al. teaches in Column 1 line 30, "an SNMP manager will periodically poll an agent 30" in order to detect changes in information for a particular network device (Column 1 lines 31-32).

It would have been obvious to one of ordinary skill in the art at the time of invention to create the invention of Ginzboorg to include "an SNMP manager will periodically poll an agent 30" as taught by Noy in order to detect changes in information for a particular network device (Column 1 lines 31-32).

Claim 3

Ginzboorg teaches the data network management system as defined in claim 1.

Ginzboorg does not specifically disclose wherein said data communication means is a Simple Network Management Protocol communication means.

However, Noy et al. teaches in Column 1 line 30, "an SNMP manager will periodically poll an agent 30" in order to detect changes in information for a particular network device (Column 1 lines 31-32).

It would have been obvious to one of ordinary skill in the art at the time of invention to create the invention of Ginzboorg to include "an SNMP manager will periodically poll an agent 30" as taught by Noy in order to detect changes in information for a particular network device (Column 1 lines 31-32).

Claim 12

Claim 12 is rejected for the same reasons as claim 2.

Claim 17

Claim 17 is rejected for the same reasons as claim 2.

(10) Response to Argument

The examiner summarizes the various points raised by the appellant and addresses the individually.

(A) Appellant Argues in regards to claims 1-20:

"The art fails to teach or suggest "a data network management system for identifying unauthorized access to a data network service..." (Appeal Brief page 13 1st paragraph) and

"Furthermore, at the location cited by the Examiner, Ginzboorg discloses that "paying customers have access to the network providing the services and the non-paying customers do not have access." In other words, non-paying or unauthorized customers "do not have access [to the network providing the services]." Since unauthorized access is expressly prohibited by Ginzboorg, Ginzboorg cannot disclose any system "for identifying unauthorized access..." (Appeal Brief page 13 4th paragraph).

In response:

The examiner respectfully disagrees with the appellant's deduction that *"Since unauthorized access is expressly prohibited by Ginzboorg, Ginzboorg cannot disclose*

any system "for identifying unauthorized access..." (Appeal Brief page 13 4th paragraph).

Ginzboorg teaches in Column 15 Lines 40-57, **"The charging functions correctly when the network access and payments are in synchronization with one another**, i.e. when the paying customers have access to the network providing the services and the non-paying customers do not have access. For example, **because of a fault the situation may sometimes change so that the router** prevents the paying customers from accessing the network providing the services or **allows access for non-paying customers** (who do not send payment CDRs). **To correct such a situation the access server polls the router and the charging server**. From the router the access server gets the access list and from the charging server the IP addresses of the customers who pay at the moment in question for access to the network. If the address of a paying customer is not included in the access list, the access server adds the address to the list. If an address included in the access list is not included in the paying customers of the charging server, the access server removes the address from the list".

Ginzboorg clearly teaches the identification of unauthorized access as shown above, specifically the disclosure "For example, **because of a fault the situation may sometimes change so that the router** prevents the paying customers from accessing the network providing the services or **allows access for non-paying customers** (who do not send payment CDRs). **To correct such a situation the access server polls the router and the charging server**" (Column 15 Lines 44-49). The examiner asserts

that at least the situation wherein the router "allows access for non-paying customers" (Column 15 Lines 44-49) constitutes an unauthorized access; therefore the teachings of Ginzboorg are analogous to the appellant's claim of "*a data network management system for identifying unauthorized access to a data network service...*" (Claim 1 first paragraph).

(B) Appellant Argues in regards to claims 1-4, 12 and 17-20:

"The art fails to teach or suggest "a data communication means for periodically polling said agent at said service node and for retrieving a user access list from said agent, said user access list specifying which users have accessed said service node..." (Appeal Brief page 14 2nd paragraph) and

"However, as discussed above, Ginzboorg's access list is a list of addresses that are permitted to access the network providing services, and is not a list of all accesses to a node or the network. Thus, the access list of G fails to teach or suggest an "access list specifying which users have accessed said service node..." as required by the quoted limitation" (Appeal Brief page 14 4th paragraph).

In response:

The examiner respectfully disagrees with the appellant's deduction that *"Ginzboorg's access list is a list of addresses that are permitted to access the network providing services, and is not a list of all accesses to a node or the network. Thus, the access list of G fails to teach or suggest an "access list specifying which users have*

accessed said service node..." as required by the quoted limitation" (Appeal Brief page 14 4th paragraph).

Ginzboorg teaches in Column 15 Lines 48-59, "To correct such a situation the access server polls the router and the charging server. **From the router the access server gets the access list** and from the charging server the IP addresses of the customers who pay at the moment in question for access to the network. If the address of a paying customer is not included in the access list, the access server adds the address to the list. **If an address included in the access list is not included in the paying customers of the charging server, the access server removes the address from the list**. The polling interval can be made to be controllable so that the access service provider can set the desired interval".

Ginzboorg clearly teaches an access list that is retrieved from the router and additionally that the access list is compared with the IP addresses retrieved from a charging server of customers who pay at the moment in question for access to the network (See above; column 15 lines 48-89). The appellant has suggested that *"Ginzboorg's access list is a list of addresses that are permitted to access the network providing services, and is not a list of all accesses to a node or the network"* (Appeal Brief page 14 4th paragraph), however it appears that the appellant has mistaken the access list of Ginzboorg for the IP addresses of paying customers, which the examiner notes are two distinct items in Ginzboorg which are compared. Since Ginzboorg teaches in Column 15 Lines 54-57 **"If an address included in the access list is not included in the paying customers of the charging server, the access server**

removes the address from the list", the examiner asserts that Ginzboorg's access list is not a list of addresses that are permitted to access the network as suggested by the appellant, but rather it is a list specifying which users have accessed said service node.

(C) Appellant Argues in regards to claims 1-4 and 5-20:

"The art fails to teach or suggest "a data processing means for detecting unauthorized access to said service node by comparing said user access list to said authorized access list..." (Appeal Brief page 15 2nd paragraph) and

"Although Ginzboorg discloses a comparison of lists, it is for the purpose of updating the access list to conform to the list of paying customers at the charging server. Ginzboorg's access list does not ever keep track of accesses to the router or the network, and so there is no way to detect whether there has been an unauthorized access. Ginzboorg is merely capable of determining that an unauthorized access was possible because of the improper inclusion of an address on the access list. Thus, Ginzboorg cannot detect an unauthorized access by comparing the two lists" (Appeal Brief page 15 5th paragraph).

In response:

The examiner respectfully disagrees.

In response to argument (A) the examiner has shown how the teachings of Ginzboorg are analogous to the appellant's claim of *"a data network management*

system for identifying unauthorized access to a data network service..." (See In response to argument (A)).

In response to argument (B) the examiner has shown that Ginzboorg's access list is not a list of addresses that are permitted to access the network as suggested by the appellant, but rather it is a list specifying which users have accessed said service node (See In response to argument (B)).

Ginzboorg teaches in Column 15 Lines 40-57, "For example, because of a fault the situation may sometimes change so that the router prevents the paying customers from accessing the network providing the services or allows access for non-paying customers (who do not send payment CDRs). **To correct such a situation the access server polls the router and the charging server. From the router the access server gets the access list and from the charging server the IP addresses of the customers who pay at the moment in question for access to the network. If the address of a paying customer is not included in the access list, the access server adds the address to the list. If an address included in the access list is not included in the paying customers of the charging server, the access server removes the address from the list**".

Ginzboorg clearly teaches the comparison of the access list to the IP addresses of the customers who pay at the moment in question for access to the network (Column 15 Lines 40-57) in order to correct the situation where the router allows access for non-paying customers, which constitutes an unauthorized access as described above in regards to argument (A).

(D) Appellant Argues in regards to claims 1-4, 6, 12, 14 and 17-20:

"The art fails to teach or suggest "a data processing means.., for updating said authorized access list based on the user access list retrieved from said agent"" (Appeal Brief page 16 1st paragraph).

In response:

The examiner respectfully disagrees.

Paragraph [0038] of the appellant's specification discloses, "Finally, in step 520, the authorized access list stored in the NMC is updated with **any access information** sent by the agent of the service node".

Ginzboorg teaches in Column 18 lines 34-46, "The volume monitoring unit VCU and the charging database BD2 used by it are included in the access server at least in the case in which it is desirable to also perform charging on the basis of a transferred volume of data. In this case the **control unit reads through the router interface unit from the router access list the desired packet counts** and **stores the data in the charging database BD2** so that **for each contract number is stored the number of packets and the IP address** used by the terminal for the connection. The access server charging database data are combined in the billing phase with the data of the charging server charging database on the basis of contract numbers. In this way it is possible to take into account the transferred data volume in the bill".

Since Ginzboorg teaches in Column15 Lines 49-52 "From the router the access server gets the access list and from the charging server the IP addresses of the customers who pay at the moment in question for access to the network" and in Column 17 lines 25-30, "FIG. 10 illustrates the structure of the charging server WD as a general level block diagram. the core of the equipment is the contract logic unit CLU2, which has access to the service database SED, the subscriber database SUD and the charging database BD", the examiner asserts that the teachings of Ginzboorg in at least Column 18 lines 37-42 "the control unit reads through the router interface unit from the router access list the desired packet counts and stores the data in the charging database BD2 so that for each contract number is stored the number of packets and the IP address used by the terminal for the connection" constitutes "*updating said authorized access list based on the user access list retrieved from said agent"* (see claim 1 4th paragraph).

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

/Farhad Ali/

Examiner, Art Unit 2446

Conferees:

/Benjamin R Bruckart/

Primary Examiner, Art Unit 2446

/Joseph E. Avellino/

Supervisory Patent Examiner, Art Unit 2458